

## Research Article

Liwei Wang, Robert Abbas, Fahad M. Almansour, Gurjot Singh Gaba, Roobaea Alroobaea, and Mehedi Masud\*

# An empirical study on vulnerability assessment and penetration detection for highly sensitive networks

<https://doi.org/10.1515/jisys-2020-0145>

received December 29, 2020; accepted March 03, 2021

**Abstract:** With the advancement of internet and the emergence of network globalization, security has always been a major concern. During the trial operation, the management control platform discussed in this article included more than 600 network security vulnerabilities in the industry, with dozens of incidents, which were promptly dealt with and rectified, effectively improving the level of network security management and protection in the industry. As networks are very much vulnerable to denial of service attacks, much more emphasis has been given to security. By improving their network security, network administrators have often tried their best. To attempt penetration testing, it is the best way of ensuring the system security. With the development of information technology, the security requirement of information system is increasing day by day. The use of penetration testing technology is conducive to the realization of accurate positioning, accurate detection, and active alarm of security vulnerabilities, and the optimization of monitoring and rectification of the combination of network security management control system. Taking penetration testing technology as one of the core elements of management and control, the risk index model is optimized to make network security management controllable and efficient, and effectively achieve management and control objectives.

**Keywords:** network globalization, security control, penetration test, network security, network administrators, security vulnerabilities, service attacks

## 1 Introduction

The rapid development of information technology makes the application of information system in various fields more common. At present, information construction in the field of education has achieved rapid development, and modern information technology has been widely applied in the education system.

---

\* **Corresponding author: Mehedi Masud**, Department of Computer Science, College of Computers and Information Technology, Taif University, Taif, KSA, e-mail: mmasud@tu.edu.sa

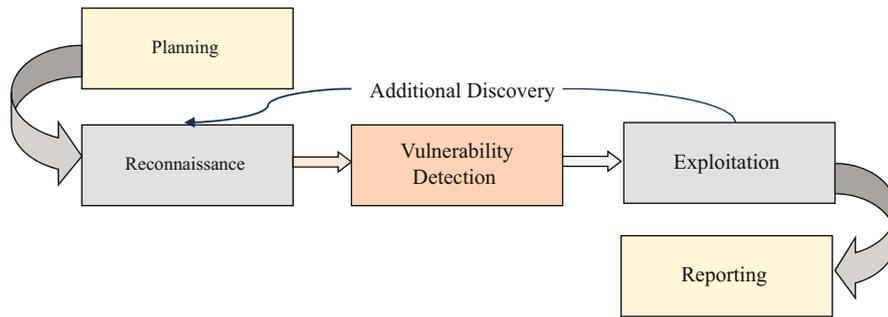
**Liwei Wang:** State Grid Hebei Electric Power Co., Ltd., Information and Communication Branch, Shijiazhuang, Hebei Province, 050000, China, e-mail: wangliwei1033@gmail.com

**Robert Abbas:** School of Engineering, Macquarie University, Macquarie Park, NSW 2113, Australia, e-mail: robert.abbas@mq.edu.au

**Fahad M. Almansour:** Department of Computer Science, College of Sciences and Arts in Rass, Qassim University, Buraydah 51452, Saudi Arabia, e-mail: f.almansour@qu.edu.sa

**Gurjot Singh Gaba:** School of Electronics and Electrical Engineering, Lovely Professional University, Phagwara 144411, India, e-mail: gurjot.17023@lpu.co.in

**Roobaea Alroobaea:** Department of Computer Science, College of Computers and Information Technology, Taif University, Taif, KSA, e-mail: r.robai@tu.edu.sa



**Figure 1:** Process of internal penetration.

For example, the use of information systems such as service portal, office automation, educational administration management, financial management, and online teaching has greatly improved work efficiency and service level [1]. Therefore, it is very important to improve the level of network security of each information system. At present, there are tens of thousands of information systems involved in the education bureau of 16 districts, more than 3,000 primary schools and kindergartens, more than 60 universities, more than 30 directly affiliated institutions, and more than 80 secondary vocational schools in Shanghai [2]. The security level of these information systems is improved to quickly find security vulnerabilities. The timely repair is one of the important means to ensure the safe operation of the systems [3]. With the rapid update of information technology, network security vulnerabilities also continue to appear. It is crucial to find security vulnerabilities in the information system's life cycle in a timely manner and quickly rectify them. Therefore, a set of effective management and control mechanism which can rely on reasonable technical means to achieve accurate location, accurate detection, active alarm, monitoring and rectification of information security management, and control system and technology platform become very necessary.

The exploits and vulnerabilities that exist within an organization are identified by the penetration testing. The security measures have been implemented by the IT infrastructure that helps the effectiveness or in-effectiveness [4–6]. The additional funding for security controls are justified in a better way as compared to the flaws present in the operational system. The penetration testing should model a real world attack that is very important [7,8]. A penetration tester will rarely be afforded this luxury, and for researching the target, a real world attacker would typically spend many months [9–11]. A similar methodology is used by the all penetration tests regardless of the actual attack profile that is being simulated. The information about a target is gained by the tester for the target acquisition. For this purpose, several ways are used such as scanning a website for names, photographs, or contact telephone numbers. Process of internal penetration is shown in Figure 1 and the example application is shown in Figure 2.

This article is structured as follows. Details of state-of-the art techniques are discussed in Section 2 followed by the contribution of the manuscript. Management control model and its elements are detailed in Section 3. Detailed controllability of explicit channels and the result analysis are presented in Section 4. Section 5 concludes the article.

## 2 Literature review

New trends in the information technology era are clouds, big data, internet of things (IoT), and artificial intelligence. Enterprises do not actively build many service-related service information systems to establish a fast and convenient connection between customers and enterprises. The author Ma, W.M. elaborates on the information security attack and defense exercises to understand the enterprise's external service information system. Hydra is a very common website penetration testing tool used by practitioners for assessing

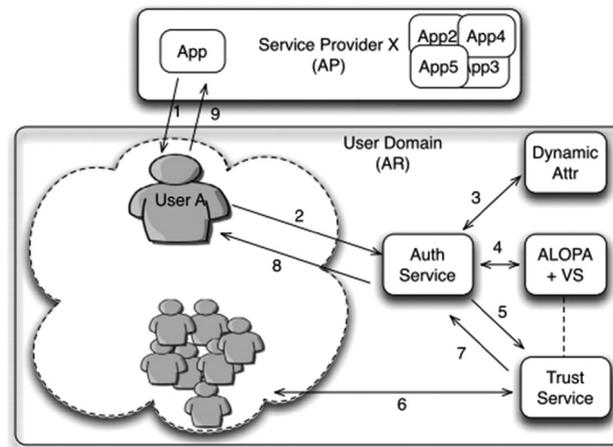


Figure 2: Example application.

vulnerabilities. Meanwhile, new investigators may gain some practical experience with website vulnerabilities, to improve their penetration ability [12,13]. Traditional machine learning algorithms have been widely used in intrusion detection, despite the scalability, functional engineering efforts, and accuracy hinder their access to safe markets. Using deep learning methods can alleviate these shortcomings, because it has been successful in the field of big data. In addition to eliminating the need for manual production, deep learning has high detection accuracy and can resist deformation attack. Diro and others propose an long short-term memory (LSTM) network for distributed network attack detection in fog-to-object communication. We identify and analyze key attacks and threats against IoT devices, in particular, the use of wireless communication vulnerabilities attack. Experiments in two cases prove that the depth model is effective and efficient than the traditional machine learning model [14]. As the private cloud spreads, protecting the network security of private cloud has become the focus of more and more enterprises. Enterprise information security system needs to integrate information security construction into infrastructure construction. The security of the enterprise private cloud network is a systematic, overall situation management engineering issue, and any private cloud vulnerability can paralyze the entire network. Qing and others take the basic network security, big data security, and private cloud network security as the starting point, analyze the relevant evaluation indexes, establish the evaluation system model and other key technologies, and expound the enterprise private cloud network security [15].

A trust enhanced distributed authorization architecture is presented by the author to provide a holistic framework [16]. The notions of “hard” and “soft” are encompassed by the model to determine whether a platform can be trusted for authorization. The hybrid model with “hard” and “soft” trust components are described after detailing the rationale for the overall model. The presented architecture is then implemented in the context of authorization for web services. The obtained results demonstrated that the presented model enables better authorization decision making, especially in a distributed environment. To manage federated authorization infrastructures, the authors of this article explore the automatic adaptation of authorization assets (policies and subject access rights). Self-Adaptive Authorization Framework (SAAF) is adapted for managing policy-based federated role/attribute that access and control authorization infrastructures [17]. A feedback loop is controlled by the SAAF controller to monitor the authorization infrastructure. A potential adaptation for handling malicious behavior is analyzed. A prototype of the SAAF controller is evaluated by the simulating malicious that demonstrating the escalation of adaptation [18]. Authorization infrastructures become increasingly difficult to manage as organizations start to federate access to their resources. The authors of this article presented a SAAF to control the access to resources through the manipulation of authorization assets that are capable of monitoring the usage of resources. The utilization of models for facilitating the autonomic management of federated authorization

infrastructures is explored by the authors. The classification is required to categorize behavior exhibited by users, including usage, for identifying abnormal behavior. Evaluation of SAAF is done by integrating it into an existing authorization infrastructure. For international information exchange and platform, network globalization and advent of internet are the main tools [19]. Networks are very much vulnerable to denial of service attacks and then much emphasis has been given to security. Network administrators have tried their best by improving their network security; however, the system is secure to attempt penetration testing. To prove whether a system is vulnerable, this is the most efficient way. By means of the internet, network security cybercrime technologies have brought many good things. There is also a criminal hacker with most technological advances [20]. Governments, companies, and private citizens are afraid that some hackers will break into their web server. The authors of this article detail the skills and attitudes of ethical hackers that how they go about helping their customers. To become an ethical hacker, which is also called as penetrate testing, there are many rules. These rules include knowledge of HTML, Java Scripts, Computer Tricks, Cracking & Breaking, etc. In this article, the authors described about the hacking techniques and the functions of how it takes place in the network.

## 2.1 Contribution

The use of penetration testing technology is conducive to the realization of accurate positioning, accurate detection, and active alarm of security vulnerabilities, and the optimization of monitoring and rectification of the combination of network security management control system are analyzed and detailed by the authors in this article. Taking penetration testing technology as one of the core elements of management and control, the risk index model is optimized to make network security management controllable and efficient, and effectively achieve management and control objectives.

## 3 Management control model and its elements

### 3.1 General model of management control

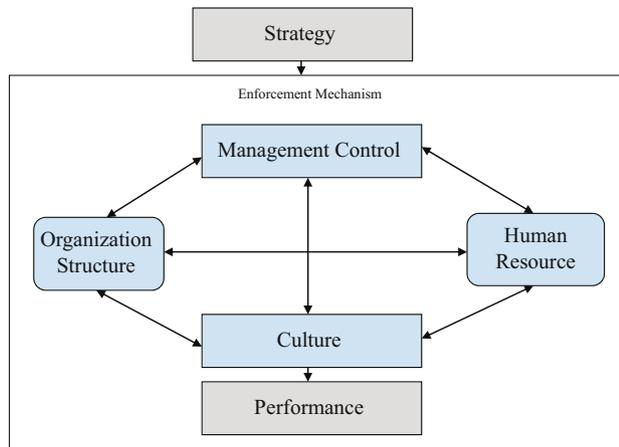
The control work in management is to determine the implementation of the plan according to the standard, and to ensure the correctness and realization of the plan objectives by correcting the deviation in the implementation.

Management control refers to the process in which managers influence other members of an organization to achieve organizational strategy. Management control process helps to achieve a desired goal, e.g., optimized and effective organization planning and coordination of normal work order and management system activities. The purpose of management control is to execute strategy (see Figure 3).

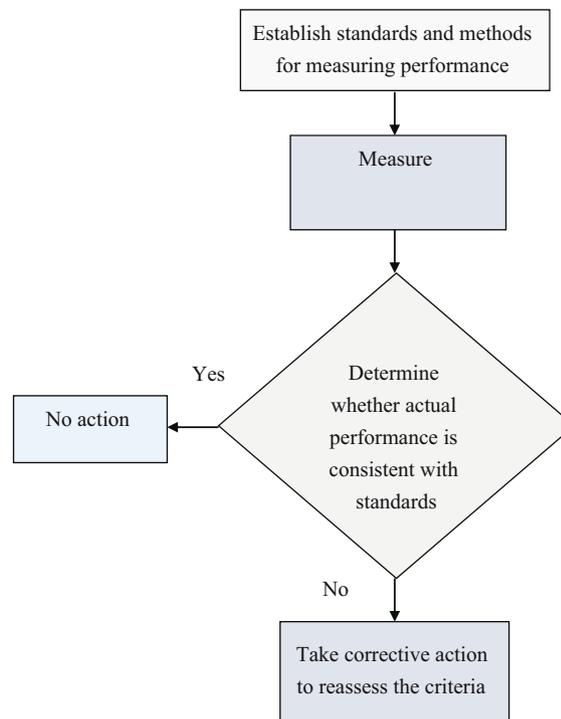
### 3.2 Management control elements

The working process of management control, as shown in Figure 4, generally consists of the following three steps: setting control objectives and establishing performance standards; measure actual work and obtain deviation information; and analyze the cause of the deviation and take corrective action (feedback control).

Feedback control is derived from the theory of automatic signal control. According to the feedback signal, it can be divided into “positive feedback” and “negative feedback.” Feedback control refers to comparing the actual results of a task after completion and judging the impact on the implementation of the next action to play a controlling role [21]. By introducing it into control science, three basic element



**Figure 3:** Management control diagram.



**Figure 4:** Controllable process of explicit channel.

nodes are set: control target, standard, deviation information, and corrective measures, which form the key node of the whole control closed-loop.

### 3.3 Penetration test

#### 3.3.1 Definition

Before we talk about penetration testing, let us talk about vulnerability scanning. Vulnerability scanning is an examination of information system security, including systems connected to the internet, applications, and online network equipment components, through the detection of vulnerabilities and security

vulnerabilities. A typical vulnerability scanner is based on a vulnerability database, which contains information about services, ports, packet types, and other known security issues that are at risk [22,23]. The risk list in the library also contains security recommendations for addressing vulnerabilities. The use of simulation hackers, malicious attack method, evaluation system security status, are used for penetration testing of a computer network system. In the whole evaluation process, the analyst takes the initiative to exploit the security vulnerability based on the location of an attacker, which is based on the active analysis of various weaknesses, technical defects, and vulnerabilities of the system. The application of penetration test to network security has become an effective technical means to prevent attacks. At the same time, we must base on the premise that the test does not affect the normal operation of the business system.

### 3.3.2 Classification

Referring to the classification of software development tests, penetration tests can be divided into the following three categories:

- (i) Black box tests, in which testers are completely ignorant of the system, perform this type of tests, and obtain information including DNS, Web, Email, and other internet services from servers that are exposed to the public by the company.
- (ii) White box test, which is the opposite to black box test. Testers can communicate with non-IT staff face to face to collect effective information, including network topology, employee information, website, and part of application code [24,25]. The purpose of the test is to simulate the operation of the staff within the enterprise.
- (iii) Covert testing, which is a test of the ability of the inspection unit to monitor, respond to, and recover information security events. Generally, when the penetration test is executed, the monitoring network personnel will monitor the changes in the network. The security management department of the unit will know the time period of the test in advance, but basically no one else knows, which is for the purpose of achieving the test better.

## 3.4 Model study

To study the network information penetration technology and penetration detection technology, we plan to establish a simulation model, which consists of the following parts: two networks with different information security levels – A network (high information security level, known controllable network) with B network (low information security level, unknown uncontrollable network); there are  $n$  known information channels between A network and B network  $e_1, e_2, \dots, e_n$ , and  $m$  unknown information channels  $h_1, h_2, \dots, h_m$ ; there are  $x$  network entities in A network  $g_1, g_2, \dots, g_x$ , including  $u$  specific information requesters  $s_1, s_2, \dots, s_u$ ; and there are  $y$  network entities in network B  $f_1, f_2, \dots, f_y$ , including  $v$  specific information publishers  $o_1, o_2, \dots, o_v$ . The specific information requester hopes to obtain specific information from the specific information publisher  $i$ , the specific information publisher wants to pass the specific information to the specific information requester, and the two transmit specific information through the specific information access flow (SIF, sensitive information flow) [26–29]. Specific information access flow has three key characteristics: specific purpose (destination), specific channel (method), and specific content (content). The information filtering system is built on  $e_1, e_2, \dots, e_n$ . The network information intrusion detection system (NIPDS) identifies and blocks the transmission of suspicious information.

**Define the following set:**

- $S$ : A collection of specific information visitors,  $S = \{s_i\}, i = 1, 2, \dots, u$ ;
- $O$ : A collection of specific information sources,  $O = \{o_i\}, i = 1, 2, \dots, v$ ;
- $E$ : Explicit information channel collection,  $E = \{e_i\}, i = 1, 2, \dots, n$ .

$E$  is divided into two subsets: the explicit controllable information channel subset  $EC$  (NIPDS can identify the information channel in  $EC$  and can be controlled) and the explicit uncontrollable information channel subset  $EU$  (NIPDS can identify the information channel in  $EU$  but unable to control or identify the specific information),  $E = EC \cup EU$ .

**Sub-definition:**  $Em = \{e_i\}, i = 1, 2, \dots, v; e_i = \langle m, oi \rangle$ ;  $ECmc = \{e_i\}, i = 1, 2, \dots, v; e_i = \langle mei = \langle mc, oi \rangle c, oi \rangle$ ;  $EUmu = \{e_i\}, i = 1, 2, \dots, v; e_i = \langle mu, oi \rangle$ ;  $mc$  is an explicit controllable access method,  $mu$  is an explicit uncontrollable access method;  $H$  is a collection of open information channels, a collection of information channels that involve human factors or are outside the scope of the current technical system processing capabilities and cannot be controlled by NIPDS:

$H = \{h_i\}, i = 1, 2, \dots, m; C$ : specific information collection,

$C = \{c_i\}, i = 1, 2, \dots, w$ . In this way, the specific information flow SIF of the research object in the penetration detection model can be abstracted into a five-tuple:

$$SIF = [S, O, E, H, C] = \{sif_i\}, \quad i = 1, 2, \dots, q$$

$$sif_i = \langle s_i, o_i, e_i, h_i, c_i \rangle, \quad s_i \in S, o_i \in O, e_i \in E, h_i \in H, c_i \in C$$

SIF can be divided into three subsets:

CSIF: Controllable specific information flow collection, where SIF adopts explicit controllable information channel, NIPDS can identify and control,

$$CSIF = [S, O, EC, H, C] \in EC \neq \phi;$$

USIF: Uncontrollable specific information flow collection, where SIF adopts explicit uncontrollable information channel, CSIF =  $[S, O, EU, H, C] \in EU \neq \phi$ ;

NSIF: Open a collection of specific information streams, where SIF uses an open information channel, CSIF =  $[S, O, f, H, C]$ . The goal of the infiltrating party (NIPT) is to make as many  $S$  as possible to obtain  $C$ , that is, to maximize the number of elements in the SIF set. As the key parameters that determine the size of SIF are the size and characteristics of  $S, O,$  and  $E$ , the infiltrator adopts micro-disordering methods to try to achieve the goal:

- (i) For a certain access method  $m_i$ , expand the controllable information channel by expanding the size of  $OEcm_i$ , makes  $sif_i \in SIFe_i$  microdisorder on  $O$ ;
- (ii) Try to use uncontrollable information channels to make  $usif_i \in USIF$  microdisorder on  $C$ ;
- (iii) Try to use open information channels to make  $nsif_i \in NSIF$  microscopic disorder in  $S, O, H, C$ . For NIPDS, the overall goal is to reduce the size of USIF and NSIF.

**Sub-goals:**

- (i) Use a man-machine system to monitor open information channels;
- (ii) Try to convert open information channels into explicit information channels, namely  $H \rightarrow EU$ ;
- (iii) Turn uncontrollable information channels into controllable information channels, from micro-disorder to macro-order, that is,  $EU \rightarrow EC$ ;
- (iv)  $csif_i \in CSIF$  from micro-controllable to macro-controllable.

That is, the information channel can be gradually monitored by the method of step-by-step degradation, and the controllability of information can be improved.

### 3.5 Monitoring of open information channels

For NIPT, the purpose is to diffuse  $C$  into all  $S$ . To achieve the above-mentioned means (1),  $O$  must be diffused to  $S$  through an open channel, so we can monitor those unknown displays by sampling. Suppose that NIPT randomly sends

$$s_i \text{ release } O_i \subset O, \text{ make } [S] = u, [O] = v.$$

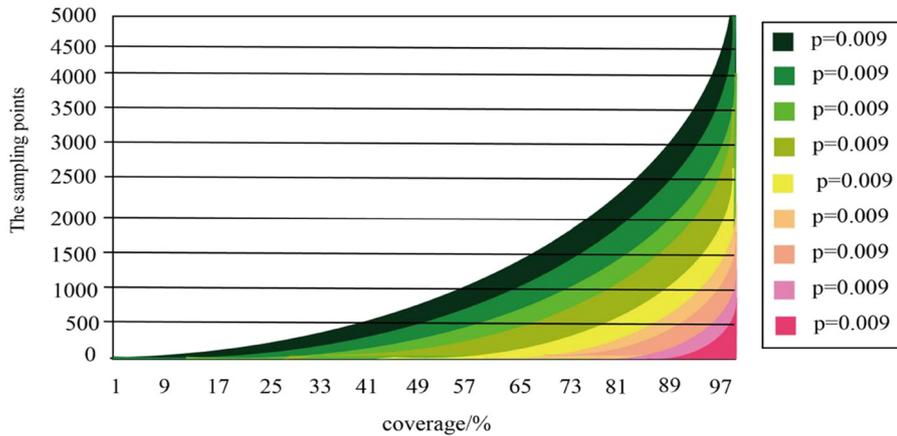


Figure 5: The  $q$ -curve cluster when  $p = 0.001 - 0.009$ .

Assume  $[O_i] = pv$ ,  $0 < p \leq 1$ , with  $q$  sampling points, wherein  $p$  is the release ratio. Besides, sampling coverage is calculated as  $r = f(p, q)$ ,  $0 < r \leq 1$ , wherein  $q$  represents sampling points. According to the principle of probability, we get

$$r_q = r_{q-1} + (1 - r_{q-1}) * p, \quad q \geq 1, \quad 0 < p \leq 1, \quad r_0 = 0. \tag{1}$$

Equation (1) can be transformed into a geometric sequence, and then according to the series formula:

$$r = 1 - (1 - p)^q, \quad q \geq 0, \quad 0 < p \leq 1. \tag{2}$$

According to equation (2), the formula for the number of sampling points can be obtained:

$$q = \ln(1 - r) / \ln(1 - p), \quad 0 < p < 1, \quad 0 < r \leq 1. \tag{3}$$

Example: set  $v = 1,000$ , random release each time  $O_i$ . The number is 3. If you want to obtain 99% coverage, the sampling point needs to be  $q = \ln(1 - 0.99) / \ln(1 - 0.003) = 1,535$ , that is, 1,535 samples need to be sampled; if  $v = 3,000$ , then  $q$  is 4,605. Another important application of equations (2) and (3) is to estimate the size of the information source  $O [O]$ . The  $q$  curve is calculated through equation (3) and presented in Figure 5 for the various values of  $p$  including  $v = 1,000$  ( $p = 0.003$ ) and  $v =$  The curve of  $q$  at 3,000 ( $p = 0.001$ ).

It can be seen that the curvatures of the two curves are different, and a graph of the  $q$  function family is obtained by setting different  $p$  values (as shown in Figure 3). Thus, sampling data can be generated after a certain amount of sampling, and the  $p$  value can be estimated by comparing the convergence curve of the published source coincidence degree of the sampling data with the  $q$  curve, thereby obtaining the approximate value of  $[O]$ . A large number of existing curve similarity calculation methods can be used for processing, and other distribution models can also be used for estimation.

## 4 Controllability of explicit channels and the result analysis

The purpose of explicit channel controllability is to analyze channels that cannot identify transmission content or protocols. The discussion on the experimentation is provided in this section.

For sequential channel transmission data (such as the content carried on SSL), if the microscopic method is still used for analysis, it will often be useless and get twice the result. It is necessary to use a higher level of macro-anomaly detection methods for analysis on massive samples, such as data stream spectrum analysis and statistical analysis. However, the current technical analysis is still developing in the direction of pure technology, and the author believes that when dealing with these problems, it is necessary

to improve the role of humans and combine humans and machines. Among them, the key issue is to establish a set of entities that have both powerful computer system support and a strong team of experts [30–33]. At the same time, they have a complete system to minimize dependence on individual people and can continue to operate without being affected by personnel in the entity [34].

A key reason why many intelligent human–machine systems established over the years have disappeared is that the system is imperfect, which makes the system unable to operate and develop sustainably. The methodology is applied to solve the open complex giant systems, such as “the comprehensive integration method from qualitative to quantitative” and “the controllable process of the explicit channel is not complicated” [35,36]. The characteristic is that the analysis process is participated in and the ability of man–machine integration is fully used, as shown in Figure 6.

**For example:** The analysis of simple unknown communication protocols can be solved by applying comprehensive integration methods:

**Put forward the proposition:** Analyze the communication law of the unknown protocol to make it macroscopically orderly and controllable.

**Raw data:** A sample of captured communication data.

**Knowledge system:** Experts’ understanding and experience of the basic laws of network communication.

**Qualitative analysis by experts:**

- (i) For simple communication protocols, if the encryption algorithm is complex, it will lead to reduced availability;
- (ii) For any application layer communication protocol, for safe transmission, there must be a signaling part, including message payload length, sequence number, verification, etc., even if it is an encryption protocol;
- (iii) Some commonly used simple encryption algorithms are known.

Perform nonlinear analysis on the sample, use the same original data multiple times, observe the results of the communication message sample, and find that the changing law of several fields, the hypothesis of each control field, and the qualitative hypothesis of the encryption method are proposed.

**Quantitative verification:** Use a large number of samples to test the coincidence rate of the hypothesis. Overturn hypotheses with counter examples, based on new evidence. Reanalyze, revise the original hypothesis, and re-verify.

**Quantitative conclusion:** To get enough macro-communication laws, it is not necessary to fully understand the details of the unknown communication protocol, but to make the communication pass programmable.

The four databases are used in this research work and 1,042 papers retrieved through the submission of the search string. Some of the papers are selected on the basis of paper’s title and abstract, and some are removed because they had no straight relation to the expected contribution. Table 1 shows the primary study for each database which is also graphically represented in Figures 7–9 for drawing better inferences.

After all that, the management control platform is also discussed in this article, which included more than 600 network security vulnerabilities in the industry during the trial operation period, and dozens of

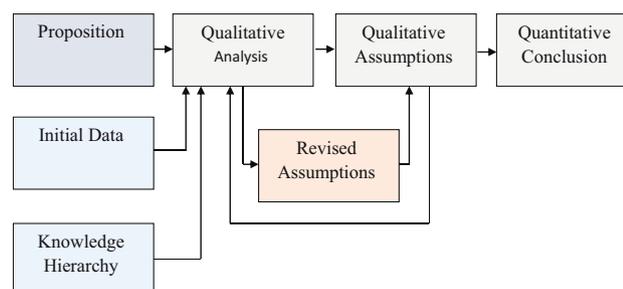
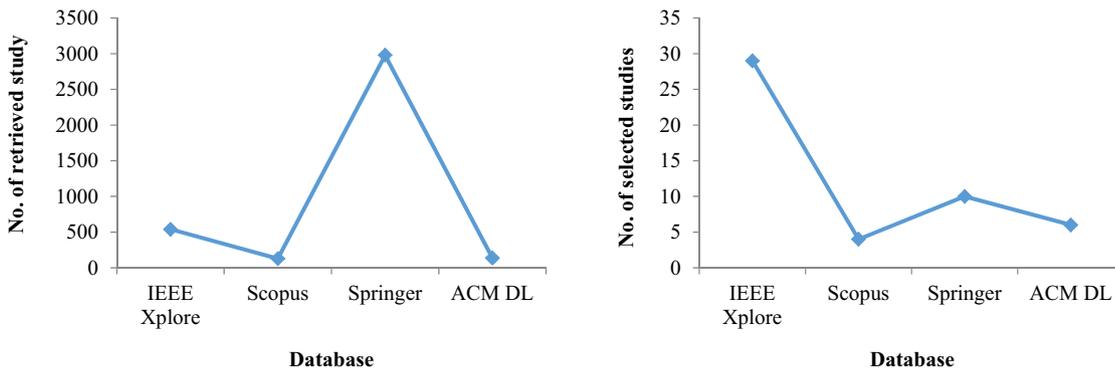


Figure 6: Controllable process of explicit channel.

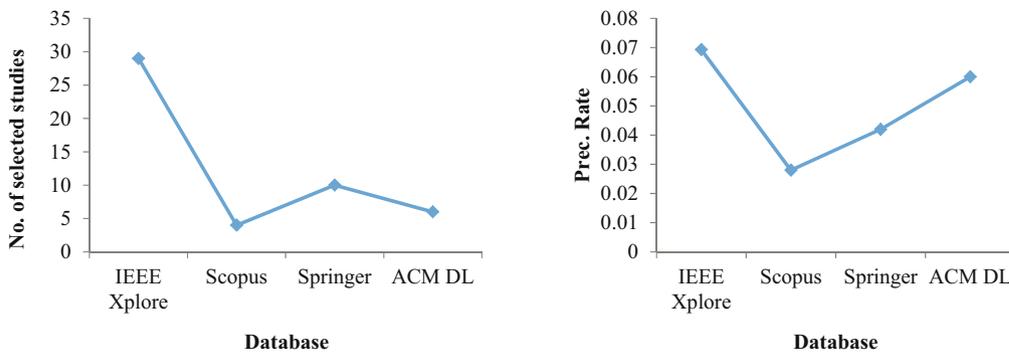
**Table 1:** Retrieved and non-duplicated and selected primary studies

| Database   | IEEE Xplore | Scopus | Springer | ACM DL |
|------------|-------------|--------|----------|--------|
| Retrieve   | 539         | 128    | 2,980    | 138    |
| Not duplic | 526         | 90     | 316      | 122    |
| Selected   | 29          | 4      | 10       | 6      |
| Prec. rate | 0.0693      | 0.028  | 0.042    | 0.06   |
| Rate index | 0.5921      | 0.051  | 0.372    | 0.52   |

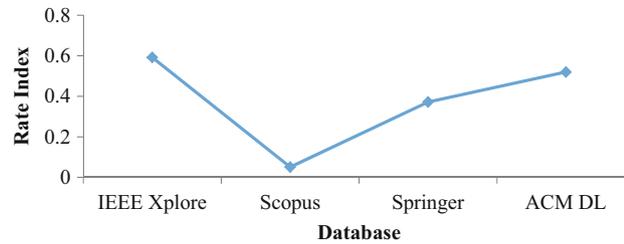
incidents were handled and rectified in a timely manner, effectively improving the industry’s network security management and protection level. Through the results of the penetration test and the performance of rectification, this article established a vulnerability risk index to quantify the vulnerability risk of each institution’s network system. By establishing a vulnerability security analysis and assessment system, timely notification, rectification, and verification of vulnerabilities can be realized, thereby effectively improving the industry’s network security management level. Through the implementation of the project, the work system of network security management and service has been strengthened, and the network security reports and processing procedures of relevant units have been standardized from the technical and administrative levels, thereby strengthening the standardization of industry network security management.



**Figure 7:** Retrieved and non-duplicated studies.



**Figure 8:** Selected criteria study and the preceding rate.



**Figure 9:** Rate index of study.

## 5 Conclusion

During the trial operation, the management control platform discussed in this article included more than 600 network security vulnerabilities in the industry, with dozens of incidents, which were promptly dealt with and rectified, effectively improving the level of network security management and protection in the industry. Through the penetration test results, this article establishes the vulnerability risk index and quantifies the vulnerability risk of each institution's network system. The use of penetration testing technology is conducive to the realization of accurate positioning, accurate detection, and active alarm of security vulnerabilities, and the optimization of monitoring and rectification of the combination of network security management control system. Through the implementation of the project, the work system of network security management and service was strengthened, and the network security report and processing process of relevant units were standardized from the technical and administrative levels, thus strengthening the standardization of network security management in the industry.

**Conflict of interest:** Authors state no conflict of interest.

## References

- [1] Xiao-Xia W. Research on information security architecture of computer network. *Digital Technol Appl.* 2018;36(12):181–2.
- [2] Dongying L, Baohai Y. Research on information security strategy based on wireless network access. *Digital Technol Appl.* 2018;36(11):191–2.
- [3] Wu YX, Wang HF. Computer network information security risks and protective measures against the background of big data. *J Luohe Vocat Tech Coll.* 2019;4:20–2.
- [4] Böhme R, Félégyházi M. Optimal information security investment with penetration testing. *International conference on decision and game theory for security.* Berlin, Heidelberg: Springer; 2010, November. p. 21–37.
- [5] Louvieris P, Clewley N, Liu X. Effects-based feature identification for network intrusion detection. *Neurocomputing.* 2013;121:265–73.
- [6] Alosaimi W, Zak M, Al-Begain K, Alroobaea R, Masud M. Economic denial of sustainability attacks mitigation in the cloud. *Int J Commun Netw Inf Security.* 2017;9(3):420–4314.
- [7] Qiu Z, Piyawattanametha W. MEMS based fiber optical microendoscopes. *Displays.* 2015;37:41–53.
- [8] SECURITIES PHOV. Management information circular; 2014.
- [9] Bacudio AG, Yuan X, Chu BTB, Jones M. An overview of penetration testing. *Int J Netw Secur Appl.* 2011;3(6):19.
- [10] Thompson HH. Application penetration testing. *IEEE Secur Priv.* 2005;3(1):66–9.
- [11] Alosaimi W, Zak M, Al-Begain K, Alroobaea R, Masud M. Mitigation of distributed denial of service attacks in the cloud. *Cybern Inf Technol.* 2017;17(14):32–5.
- [12] Yeo J. Using penetration testing to enhance your company's security. *Comput Fraud Secur.* 2013;2013(4):17–20.
- [13] Ma WM. Research on website penetration test. *Glob Bus Manag J.* 2019;11:121–32.
- [14] Diro A, Chilamkurti N. Leveraging LSTM networks for attack detection in fog-to-things communications. *IEEE Commun Mag.* 2018;56(9):124–30.
- [15] Qing L, Boyu Z, Jinhua W, Qinqian L. Research on key technology of network security situation awareness of private cloud in enterprises. In *2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA).* IEEE; 2018. pp. 462–6.

- [16] Nagarajan A, Varadharajan V, Tarr N. Trust enhanced distributed authorisation for web services. *J Comput Syst Sci.* 2014;80(5):916–34.
- [17] Bailey C, Chadwick DW, de Lemos R. Self-adaptive federated authorization infrastructures. *J Comput Syst Sci.* 2014;80(5):935–52.
- [18] Bailey C. Application of self-adaptive techniques to federated authorization models. 2012 34th international conference on software engineering (ICSE). IEEE; 2012, June. p. 1495–8.
- [19] Budiarto R, Ramadass S, Samsudin A, Noor S. Development of penetration testing model for increasing network security. *Proceedings 2004 international conference on information and communication technologies: from theory to applications, 2004.* IEEE; 2004, April. p. 563–4.
- [20] Shanmugapriya R. A study of network security using penetration testing. 2013 international conference on information communication and embedded systems (ICICES). IEEE; 2013, February. p. 371–4.
- [21] Zhou D. Research on the security strategy and technology of information resource network of chinese academy library. *J Phys Conf Ser.* 2020;1550:032037.
- [22] Duan T, Xiang J, Zhang H, Li Q-M. Research on simulation method of industrial control system attack based on hybrid test. *Cyber Secur.* 2019;3:8–22.
- [23] Zhou D. Research on the security strategy and technology of information resource network of chinese academy library. *J Phys Conf Ser.* 2020;1550:032037.
- [24] Kumar D, Sharma A, Kumar R, Sharma N. Restoration of the network for next generation (5G) optical communication network. In 2019 International Conference on Signal Processing and Communication (ICSC). IEEE; 2019. pp. 64–8.
- [25] Sharma A. Optical sensors in environmental applications. *Environmental and process monitoring technologies.* Vol. 1637. International Society for Optics and Photonics; 1992, May. p. 270–9.
- [26] Rathee G, Sharma A, Kumar R, Ahmad F, Iqbal R. A trust management scheme to secure mobile information centric networks. *Comput Commun.* 2020;151:66–75.
- [27] Zhan W, Tao Z. Research on 5G mobile communication network security technology. *J Phys Conf Ser.* 2020;1634(1):012055 (7pp).
- [28] Mehedi M, Shamim H. Secure data-exchange protocol in a cloud-based collaborative health care environment. *Multimed Tools Appl.* 2020;77(9):11121–35.
- [29] Sharma A, Kumar R. A framework for pre-computed multi-constrained quickest qos path algorithm. *J Telecommun Electron Computer Eng (JTEC).* 2017;9(3–6):73–7.
- [30] Sharma A, Ansari MD, Kumar R. A comparative study of edge detectors in digital image processing. In 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC). IEEE; 2017. pp. 246–50.
- [31] Kumar R, Kumar P. Special issue on recent trends in artificial intelligence techniques for fault-tolerance, reliability and availability in mission-critical networks. *Recent Adv Comput Sci Commun (Formerly: Recent Pat Comput Sci).* 2020;13(3):311–2.
- [32] Passarella A. A survey on content-centric technologies for the current Internet: CDN and P2P solutions. *Comput Commun.* 2012;35(1):1–32.
- [33] Dogra J, Jain S, Sharma A, Kumar R, Sood M. Brain tumor detection from MR images employing fuzzy graph cut technique. *Recent Adv Comput Sci Commun (Formerly: Recent Pat Comput Sci).* 2020;13(3):362–9.
- [34] Huang HC, Zhang ZK, Cheng HW, Shieh SW. Web application security: threats, countermeasures, and pitfalls. *Computer.* 2017;50(6):81–5.
- [35] Khan R, Kumar P, Jayakody DNK, Liyanage M. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *IEEE Commun Surv Tutor.* 2019;22(1):196–248.
- [36] Borrión H, Amiri A, Delpech D, Lemieux AM. Experimental assessment of the viability of using ground penetrating radar for metal wire-snare detection. *Crime Sci.* 2019;8(1):1–10.